

Formal Verification of a Parameterized Data Aggregation Protocol

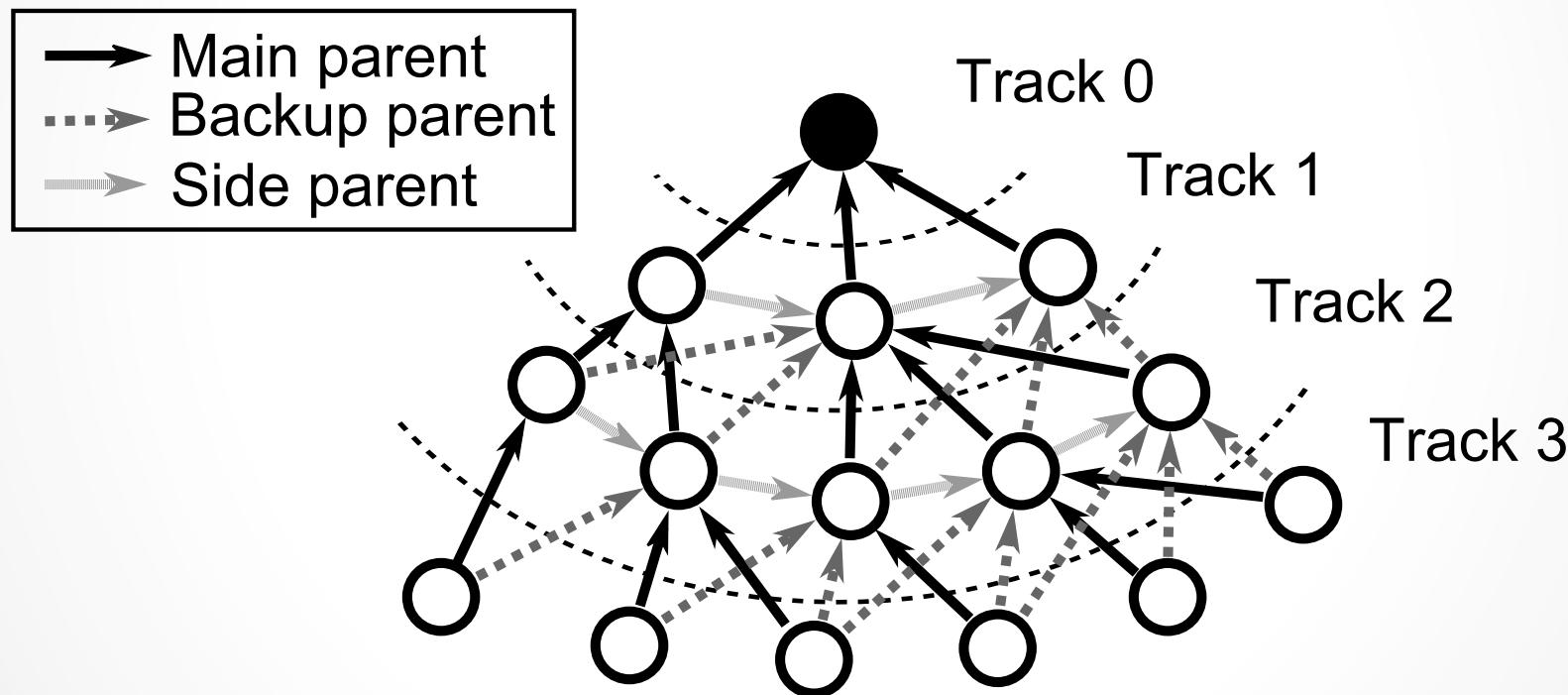
Sergio Feo-Arenis, Bernd Westphal



Aggregation Protocols



Aggregation Protocols



Verification Problem

INPUT:

- Aggregation Algorithm
- Topology Constraints

WITH:

- Unreliable Links

“In all possible system configurations, does the protocol perform aggregation correctly?”

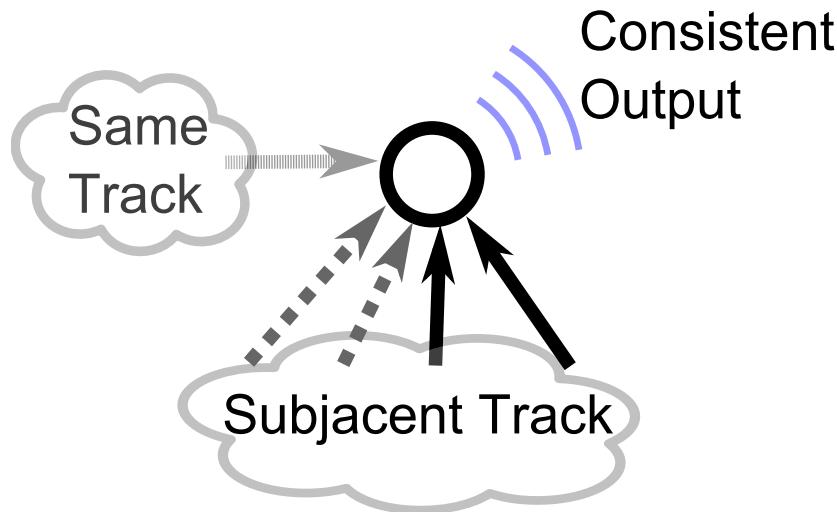


What is in the Paper?

- Formalization of the System:
Axiomatization of Topologies,
Schedules and Links
 - Formalization of the
correctness property
- •

What is in the Paper?

- Reduction of the correctness property to a local one.



- Can be checked(semi) automatically

What is in the Paper?

- Check the axiomatization using Isabelle
- Check local correctness using Boogie
- Inductive proof:

From local consistency to protocol correctness

